デスクトップ マネジメントについて
Business Desktop

製品番号：312947-292

2003年9月

このガイドでは、一部のモデルにプリインストールされているセキュリティ機能とインテリジェント マネジメント機能の概念および使用手順について説明します。

本製品は、日本国内で使用するための仕様になっており、日本国外で使用される場合は、仕様の変更を必要とすることがあります。

本書に記載されている製品情報は、日本国内で販売されていないものも含まれている場合があります。

以下の記号は、本文中で安全上重要な注意事項を示します。

警告：その指示に従わないと、人体への傷害や生命の危険を引き起こす恐れがあるという警告事項を表します。

注意：その指示に従わないと、装置の損傷やデータの損失を引き起こす恐れがあるという注意事項を表します。

デスクトップ マネジメントについて
Business Desktop
改訂第1版 2003年9月
初版 2003年3月
製品番号：312947-292

日本ヒューレット・パッカード株式会社

目次

デスクトップ マネジメント

索引

デスクトップ マネジメント

HPのインテリジェント マネジメント機能は、ネットワーク環境にあるデスクトップ、ワークステーション、およびノートブック コンピュータの管理と制御の分野で、標準のソリューションを提供しています。HPはデスクトップ マネジメントのパイオニアとして1995年に、デスクトップを完全に管理できる業界初のパーソナル コンピュータを世に送り出しました。HPはマネジメント機能の特許を取得しています。以来、デスクトップ、ワークステーション、およびノートブック コンピュータの効果的な導入、設定、および管理に必要な標準化とインフラストラクチャの開発において業界全体の取り組みをリードしてきました。HPは、業界トップ クラスの管理ソフトウェア ソリューション提供企業との提携関係により、これらの企業の製品とインテリジェント マネジメント機能の互換性を確保しています。インテリジェント マネジメント機能は、ライフサイクル ソリューションを提供する幅広い取り組みの中でも重要な位置を占めるもので、デスクトップ コンピュータのライフサイクルの4つの側面である計画、導入、管理、移行でユーザをサポートします。

デスクトップ マネジメントの主要な機能と特長は、次のとおりです。

- 出荷時設定の変更
- リモート システム インストール
- ソフトウェア アップデートおよびマネジメント機能
- ROMフラッシュ
- 資産情報管理機能およびセキュリティ機能
- 障害通知および復旧機能

このガイドで説明される機能のサポートについては、機種またはソフトウェアのバージョンにより異なることがあります。

出荷時設定の変更

お使いのコンピュータには、システム ソフトウェア イメージがプリインストールされています。ソフトウェアの設定手順を簡単に済ませると、すぐにコンピュータを使用できます。

プリインストールされたソフトウェア イメージの代わりにカスタマイズされたシステム ソフトウェアおよびアプリケーション ソフトウェアを使うこともできます。カスタマイズされたソフトウェア イメージを展開するには、いくつかの方法があります。

- プリインストールされたソフトウェア イメージを展開した後、追加するアプリケーションをインストールする。
- Altiris Deployment Solutionsなどのソフトウェアの導入用ツールを使用して、プリインストール ソフトウェアの代わりにカスタマイズされたソフトウェア イメージを使用する。
- ディスク複製手順を使用して、ハードディスク ドライブの内容を別のハードディスクにコピーする。

最適なコンピュータ環境の構築方法は、お使いになる情報技術内容や作業内容によって異なります。HPライフサイクル ソリューションに関する弊社のホームページ（http://h18000.www1.hp.com/solutions/pcsolutions、英語サイト）には、お使いの環境に適したコンピュータの導入方法を選択する際に役立つ情報が掲載されています。

Restore Plus! CD、ROMからのセットアップ、およびACPIハードウェアにより、システム ソフトウェアのリストア、コンフィギュレーション マネジメント機能、トラブルシューティング、および省電力機能を利用することができます。

リモート システム インストール

Preboot Execution Environment（PXE）を起動すれば、リモート システム インストールを使用してネットワーク サーバからソフトウェアやコンフィギュレーション情報（コンピュータの設定情報）を取り出して、コンピュータを起動したりセットアップしたりすることができます。リモート システム インストールの機能は、通常、システム セットアップやコンフィギュレーションのためのツールとして使用しますが、次のような場合にも使用できます。

- ハードディスク ドライブをフォーマットするとき
- 1台以上の新しいコンピュータにソフトウェア イメージを導入するとき
- フラッシュ ROMを使用してシステムBIOSをリモートでアップデートするとき（9ページの「リモートROMフラッシュ機能」を参照）
- システムBIOSを設定するとき

リモート システム インストールを起動するには、起動時に表示されるHPロゴの画面の右下隅に[F12 = Network Service Boot]と表示されたら、すぐに**[F12]**キーを押します。画面のメッセージに従って、リモート システム インストールを起動します。デフォルトの起動順序はBIOSのコンフィギュレーションの設定ですが、常にPXEを起動するように変更できます。

HPとAltiris社の提携により、企業におけるコンピュータの導入と管理を短時間で容易に実行できるツールが開発されました。このツールを使用すると、TCO（維持管理費）が大幅に削減されます。HPのコンピュータが、企業環境内で最も管理しやすいクライアント マシンになります。

ソフトウェアのアップデートと管理

HPでは、デスクトップ コンピュータおよびワークステーションのソフトウェアを管理し、アップデートするためのツール（Altiris、Altiris PC Transplant Pro、Altirisのソリューションである HP Client Manager Software、System Software Manager、Proactive Change Notification（製品変更通知）、およびActiveUpdate）を提供しています。

HP Client Manager Software

HP Client Manager Software（HP CMS）はAltiris内でHPのインテリジェント マネジメント機能を強力に統合し、HPのアクセス デバイスに以下のような優れたハードウェア管理機能を提供します。

- 資産管理用のハードウェア インベントリの詳細表示
- コンピュータの状態検査の監視および診断
- ハードウェア環境の変化についての事前通知
- マシン温度についての警告、メモリ異常の警告など、企業活動における重大な状況についての、Webサイトを利用した報告
- システム ソフトウェア（デバイス ドライバやROM BIOSなど）のリモート アップデート
- 起動順序のリモートからの変更

HP Client Managerについて詳しくは、http://h18000.www1.hp.com/im/client_mgr.html（英語サイト）を参照してください。

Altiris Solutions

HP Client Manager Solutionでは、HPクライアント デバイスのハードウェアの中央管理機能が、すべてのITライフサイクル分野に提供されます。

- 資産管理
  - ソフトウェア ライセンスの準拠
  - コンピュータの管理および報告
  - リース契約および固定資産の管理
- 展開と移行
  - Microsoft Windows 2000、Windows XP Professional、またはHome Editionへの移行
  - システムの展開
  - 個人設定の移行
- ヘルプデスクと問題解決
  - ヘルプデスク チケットの管理
  - リモートでのトラブルシューティング
  - リモートでの問題解決
  - クライアントでの問題修復
- ソフトウェアおよび操作の管理
  - デスクトップ マネジメントの実行
  - HPシステム ソフトウェアの展開
  - アプリケーションの自己修復

一部のデスクトップおよびノートブック コンピュータには、工場出荷時にロードされたイメージの1つとしてAltirisマネジメント エージェントが含まれています。このエージェントによりAltiris Development Solutionsとの通信が可能になります。Altiris Development Solutionsを使用すると、簡単なウィザードに従って、新しいハードウェアの展開や新しいオペレーティング システムへの個人設定の移行を完了することができます。Altiris Solutionsソフトウェアには、使いやすいソフトウェア配布機能も含まれています。System Software ManagerまたはHP Client Managerと組み合わせて使用すると、管理者はROM BIOSとデバイス ドライバのソフトウェアを中央管理コンソールからアップデートすることもできます。

詳しくは、HPのWebサイト、http://www.hp.com/go/easydeploy（英語サイト）を参照してください。

Altiris PC Transplant Pro

Altiris PC Transplant Proを使用すると、既存の設定、ユーザ設定、およびデータを保存し、新しい環境に迅速かつ簡単に移行することができます。アップグレードは何日も何時間もかからず分単位で済み、移行後のデスクトップは、外観も動きもユーザの期待どおりになります。

詳細情報および30日間試用版のダウンロード方法については、http://h18000.www1.hp.com/im/prodinfo.html#deploy（英語サイト）を参照してください。

System Software Manager

System Software Manager（SSM）は、複数のシステムにおいてシステム レベルのソフトウェアを同時にアップデートできるユーティリティです。SSMは、コンピュータのクライアント システムで使用すると、ハードウェアおよびソフトウェアのバージョンを検出し、ファイル格納ディレクトリと呼ばれる中央のリポジトリから適切なソフトウェアをアップデートします。SSM でサポートされるドライバのバージョンは、ドライバのダウンロード サイトおよびサポート ソフトウェアCDに、独自のアイコンで示されています。ユーティリティのダウンロードまたはSSMについて詳しくは、http://h18000.www1.hp.com/im/ssmwp.html（英語サイト）を参照してください。

Proactive Change Notification

Proactive Change Notificationプログラムは、Subscriber's ChoiceのWebサイトを利用して、以下のことを事前にかつ自動的に行います。

- ほとんどの企業向けHP製コンピュータおよびサーバでハードウェアおよびソフトウェアの変更があった場合に、最も早くて60日前に電子メールでProactive Change Notification（PCN）を通知する
- ほとんどの企業向けHP製コンピュータおよびサーバについてのCustomer Bulletins、Customer Advisories、Customer Notes、Security Bulletins、およびDriver alertsを含んだ電子メールを送信する

特定のIT環境に該当する情報のみを受け取るようにするため、ユーザ専用のプロファイルを作成します。Proactive Change Notificationプログラムおよびカスタム プロファイルの作成方法について詳しくは、http://www.hp.com/go/pcn（英語サイト）を参照してください。

ActiveUpdate

ActiveUpdateはHPのクライアントベースのアプリケーションです。ActiveUpdate クライアントはユーザのローカル システムで稼動し、ユーザ定義のプロファイルを使用して、ほとんどの企業向けHPコンピュータおよびサーバに関連するソフトウェアのアップデート版を事前にかつ自動的にダウンロードします。ダウンロードした最新ソフトウェアは、HP Client Manager SoftwareおよびSystem Software Managerが対象とするコンピュータに適切に展開されます。

ActiveUpdate、アプリケーションのダウンロード、およびカスタム プロファイルの作成方法について詳しくは、http://h18000.www1.hp.com/products/servers/management/activeupdate/index.html（英語サイト）を参照してください。

ROMフラッシュ機能

お使いのコンピュータでは、オペレーティング システムとの情報のやりとりなどを行う基本入出力システム（BIOS）がプログラム可能なフラッシュROMに記憶されているので、必要に応じて簡単にアップグレードすることができます。ROMのアップグレードにはRomPaqディスケットが必要です。RomPaqディスケットは、インターネットのHPホームページからダウンロードできます。ROMのアップグレード手順については、RomPaqディスケットに付属の説明を参照してください。

注意：コンピュータにセットアップ パスワードを設定しておけば、システムROMの内容が不用意に変更されるのを防ぐことができます。コンピュータにセットアップ パスワードが設定されていないと、ROMへの書き込みが禁止されていないので、不用意にROMの内容が変更されてしまう危険があります。

システムROMのバージョンがお使いのコンピュータのモデルやオペレーティング システムに合っていないと、コンピュータが正しく動作しないことがあります。

System Software Managerを使用すると、システム管理者が、複数のコンピュータに同時にセットアップ パスワードを設定することができます。

詳しくは、http://h18000.www1.hp.com/im/ssmwp.html（英語サイト）を参照してください。

リモートROMフラッシュ機能

リモートROMフラッシュ機能を利用すれば、システム管理者は、ネットワーク管理端末からリモートでコンピュータのROMを安全に書き換えることができます。複数のHPのコンピュータに対してこのような作業をリモートで行うことができるので、ネットワーク上のコンピュータのROMを適切にアップグレードし、少ない費用で管理することができます。

リモートROMフラッシュを使用するには、リモート ウェイク アップ機能を使って、お使いのコンピュータの電源を入れておくか、再起動しておく必要があります。

リモートROMフラッシュについて詳しくは、http://h18000.www1.hp.com/im/prodinfo.html（英語サイト）でHP Client Manager SoftwareまたはSystem Software Managerについての説明を参照してください。

HPQFlash

HPQFlashユーティリティは、Windowsオペレーティング システムで個別のコンピュータ上でシステムROMのアップデートや復元を行う場合に使用します。

HPQFlashについて詳しくは、http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html（英語サイト）を参照してください。

ブート ブロックROM

ブート ブロックROMが装備されているので、システムROMのアップグレード中に電源の障害が発生するなどしてROMの書き換えに失敗した場合も、システムROMを復旧またはアップグレードすることができます。ブート ブロックはROMフラッシュの際にも更新されない領域に収められており、コンピュータの電源が入れられるたびにシステムROMフラッシュをチェックし、以下のどれかの方法でコンピュータを起動します。

- システム ROM が有効な場合は、コンピュータは通常の方法で起動します。
- システムROMが有効でない場合は、システムROMの復旧作業を実行できるように、RomPaqディスケットからのコンピュータの起動を、ブートブロックROMがサポートします。

ブート ブロックROMによりシステムROMが有効でないことが検出されると、システム電源ランプが8回赤く点滅し（1秒間に1回点滅した後に2秒間休止）、同時にビープ音が8回鳴ります。ブート ブロックのリカバリ モードのメッセージが、画面に表示されます（一部のモデルのみ）。

ブート ブロックのリカバリ モードになったら、以下のように操作して、システムROMを復旧（アップグレード）してください。

1. ディスケット ドライブにディスケットが入っている場合は取り出し、コンピュータの電源を切ります。
2. RomPaqディスケットをディスケット ドライブに挿入します。
3. コンピュータの電源を入れます。
4. RomPaqディスケットが認識されない場合、RomPaqディスケットを挿入してコンピュータを再起動するように指示されます。
5. セットアップ パスワードが設定されている場合、Caps Lockランプが点灯し、パスワード入力を求められます。
6. セットアップ パスワードを入力します。
7. RomPaqディスケットからの再起動が正しく行われ、システムROMの復旧またはアップグレードが正常に完了すると、キーボード上の3つのランプが点灯し、ビープ音が鳴ります。
8. ディスケットを取り出して電源を切ります。

9. 電源を入れなおして、コンピュータを起動します。

次の表に、ブート ブロックROMによるさまざまなキーボード ランプの状態（コンピュータにPS/2キーボードが接続されている場合）を示します。また、各ランプの状態の意味およびランプの状態に応じて行う操作も示します。

ブート ブロックROM**によるキーボード ランプの状態**

ブート ブロック モード	ランプの色	ランプの状態	意味
Num Lock	緑色	オン	RomPaqディスケットが挿入されていないか、壊れているか、またはドライブが正常に動作していない
Caps Lock	緑色	オン	パスワードを入力してください
Num、Caps、Scroll Lock	緑色	Num Lock、Caps Lock、Scroll Lockの順に1個ずつ点滅	キーボードがネットワーク モードでロックされた
Num、Caps、Scroll Lock	緑色	オン	ブート ブロックROMフラッシュが完了した。コンピュータの電源を入れなおして、コンピュータを再起動してください

診断ランプは、USBキーボードでは点滅しません。

リプリケート セットアップ機能

以下のリプリケート セットアップ機能を使用すれば、コンピュータの設定情報(コンフィギュレーション情報)を他の同じモデルのコンピュータにコピーすることができます。この機能によって、複数のコンピュータに同じ設定を行う時間を短縮することができます。

これらの手順を行うには、ディスケット ドライブ、またはHP USBメモリなどのサポートされるUSBフラッシュ メディア デバイスが必要です。

1台のコンピュータへのコピー

注意：設定情報はモデルにより異なります。コピー元とコピー先のコンピュータが別のモデルの場合、ファイル システムが破損する恐れがあります。たとえば、D510 USからD510 e-pcに設定情報をコピーしないでください。

1. コピーする設定情報を選択して、コンピュータを起動または再起動します。Windowsを実行している場合は、**[スタート]→[終了オプション]**（または**[シャットダウン]**）→**[コンピュータを再起動する]**（または**[再起動する]**）の順に選択します。
2. モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータの電源をいったん切ってから入れなおして、もう一度**[F10]**キーを押してください。

3. ディスケットまたはUSBフラッシュ メディア デバイスを挿入します。
4. **[ファイル]**（File）→**[ディスケットに保存]**（Save to Diskette）の順に選択します。画面上のメッセージに従って操作し、設定情報ディスケットまたはUSBフラッシュ メディア デバイスを作成します。
5. 設定するコンピュータの電源を切り、設定情報ディスケットまたはUSBフラッシュ メディア デバイスを挿入します。
6. 設定するコンピュータの電源を切ります。モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

7. **[ファイル]**（File）→**[システム構成の復元]**（Restore from Diskette）の順に選択したあと、画面上のメッセージに従って操作します。
8. 設定が完了したら、コンピュータを再起動します。

複数のコンピュータへのコピー

注意：設定情報はモデルにより異なります。コピー元とコピー先のコンピュータが別のモデルの場合、ファイル システムが破損する恐れがあります。たとえば、D510 USからD510 e-pcに設定情報をコピーしないでください。

この手順では設定情報ディスケットまたはUSBフラッシュ メディア デバイスの作成に少し時間がかかりますが、設定情報をコピー先のコンピュータにコピーする時間は大幅に短縮されます。

Windows 2000では起動可能ディスケットを作成できません。この手順を行うため、および起動可能USBフラッシュ メディア デバイスを作成するためには、起動可能ディスケットが必要です。起動可能ディスケットを作成するためにWindows 9xまたはWindows XPを使用できない場合は、1台のコンピュータへのコピーの手順を実行してください（12ページの「1台のコンピュータへのコピー」を参照してください）。

1. 起動可能ディスケットまたはUSBフラッシュ メディア デバイスを作成します。14ページの「起動可能ディスケット」、15ページの「サポートされるUSBフラッシュ メディア デバイス」、または18ページの「サポートされないUSBフラッシュ メディア デバイス」を参照してください。

注意：USBフラッシュ メディア デバイスから起動できないコンピュータもあります。コンピュータ セットアップ（F10）ユーティリティに表示されるデフォルトの起動順序で、USBデバイスがハードディスク ドライブより前にある場合、そのコンピュータはUSBフラッシュ メディア デバイスから起動できます。それ以外の場合は、起動可能ディスケットを使用してください。

2. コピーする設定情報を選択して、コンピュータを起動または再起動します。Windowsを実行している場合は、**[スタート]**→**[終了オプション]**（または**[シャットダウン]**）→**[コンピュータを再起動する]**（または**[再起動する]**）の順に選択します。

3. モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータの電源をいったん切ってから入れなおして、もう一度**[F10]**キーを押してください。

4. 起動可能ディスケットまたはUSBフラッシュ メディア デバイスを挿入します。
5. **[ファイル]**（File）→**[ディスケットに保存]**（Save to Diskette）の順に選択します。画面上のメッセージに従って操作し、設定情報ディスケットまたはUSBフラッシュ メディア デバイスを作成します。
6. リプリケート セットアップ機能があるBIOSユーティリティ（repset.exe）をダウンロードして、設定情報ディスケットまたはUSBフラッシュ メディア デバイスにコピーします。このユーティリティは、http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html からダウンロードできます。
7. 設定情報ディスケットまたはUSBフラッシュ メディア デバイス上で、次のコマンドを含むautoexec.batファイルを作成します。

   repset.exe
8. 設定するコンピュータの電源を切ります。設定情報ディスケットまたはUSBフラッシュ メディア デバイスを挿入し、コンピュータの電源を入れます。設定ユーティリティが自動的に実行されます。
9. 設定が完了したら、コンピュータを再起動します。

起動可能デバイスの作成

起動可能ディスケット

以下の手順はWindows XP ProfessionalおよびHome Editionに対応しています。Windows 2000では起動可能ディスケットを作成できません。

1. ディスケットをディスケット ドライブに挿入します。
2. **[スタート]**→**[マイ コンピュータ]**の順に選択します。
3. ディスケット ドライブを右クリックして、**[フォーマット]**をクリックします。

4. [MS-DOSの起動ディスクを作成する]チェック ボックスをオンにして、[開始]をクリックします。

13ページの「複数のコンピュータへのコピー」に戻ります。

サポートされるUSBフラッシュ メディア デバイス

HP USBメモリなどのサポートされるデバイスには、そのデバイスを簡単な手順で起動可能にするためのイメージがプリインストールされています。使用しているUSBメモリにこのイメージが存在しない場合は、後で説明する手順に従ってください（18ページの「サポートされないUSBフラッシュ メディア デバイス」を参照してください）。

注意：USBフラッシュ メディア デバイスから起動できないコンピュータもあります。コンピュータ セットアップ（F10）ユーティリティに表示されるデフォルトの起動順序で、USBデバイスがハードディスク ドライブより前にある場合、そのコンピュータはUSBフラッシュ メディア デバイスから起動できます。それ以外の場合は、起動可能ディスケットを使用してください。

起動可能なUSBフラッシュ メディア デバイスを作成するには、次のものが必要です。

- 次のうち1つのコンピュータ
  - Compaq Evo D510 US
  - Compaq Evo D510 MT/SF
  - HP Compaq Business Desktop d530シリーズ：US、SF、またはMT
  - Compaq Evo N400c、N410c、N600c、N610c、N620c、N800c、またはN1000cノートブック コンピュータ
  - Compaq Presario 1500または2800ノートブック コンピュータ

  BIOSによっては、将来リリースされるコンピュータでもHP USBメモリからの起動がサポートされる場合があります。

注意：上記以外のコンピュータを使用している場合は、コンピュータ セットアップ（F10）ユーティリティに表示されるデフォルトの起動順序で、USBデバイスがハードディスク ドライブより前にあることを確認してください。

■ 次のうち1つのストレージ モジュール

- ❏ 16MB HP USBメモリ
- ❏ 32MB HP USBメモリ
- ❏ 64MB HP USBメモリ
- ❏ 128MB HP USBメモリ

■ FDISKおよびSYSプログラムが格納された、起動可能なDOSディスケット。SYSがない場合はFORMATを使用できますが、USBメモリ上のファイルがすべて失われます。

1. コンピュータの電源を切ります。
2. USBメモリをコンピュータのUSBポートのどれかに差し込み、USBディスケット ドライブ以外のすべてのUSBストレージ デバイスを取り外します。
3. FDISK.COMと、SYS.COMまたはFORMAT.COMのどちらかが格納された起動可能なDOSディスケットをディスケット ドライブに挿入します。コンピュータの電源を入れて、DOSディスケットを起動します。
4. A:¥プロンプトで「**FDISK**」と入力して**[Enter]**キーを押し、FDISKを実行します。メッセージが表示されたら、[Yes (Y)]をクリックして大容量ディスクのサポートを有効にします。
5. 選択肢の「**5**」を入力してコンピュータのドライブを表示します。一覧のドライブに最も近いドライブはUSBメモリで、通常は一覧の最後に表示されます。ドライブ名を書き留めておきます。

   USBメモリのドライブ名：_____

△ **注意：**ドライブがUSBメモリと一致しない場合は、データの損失を防ぐため、次の手順に進まないでください。他にストレージ デバイスがないか、すべてのUSBポートを確認します。あった場合は取り外してコンピュータを再起動し、手順4に進みます。ない場合、コンピュータがUSBメモリに対応していないか、USBメモリが破損しています。この場合はUSBメモリを起動可能にするための手順を実行しないでください。

6. **[Esc]**キーを押してA:¥プロンプトに戻り、FDISKを終了します。
7. 起動可能なDOSディスケットにSYS.COMがある場合は手順8に、ない場合は手順9に進みます。
8. A:¥プロンプトで「**SYS x:**」（**x**は書き留めたドライブ名）と入力し、手順13に進みます。

注意：USBメモリのドライブ名を正しく入力したことを確認します。

システム ファイルの転送が完了すると、SYSからA:¥プロンプトに戻ります。

9. 保存しておきたいファイルをUSBメモリから別のドライブ（コンピュータの内蔵ハードディスク ドライブなど）の一時ディレクトリにコピーします。
10. A:¥プロンプトで「**FORMAT /S X:**」（**x**は書き留めたドライブ名）と入力します。

注意：USBメモリのドライブ名を正しく入力したことを確認します。

FORMATでは1つ以上の警告が表示され、次の手順に進む前に毎回確認画面が表示されます。毎回「**y**」と入力します。FORMATによりUSBメモリがフォーマットされ、システム ファイルが追加され、ボリューム ラベルが要求されます。

11. ラベルを付けない場合は**[Enter]**キーを押し、必要な場合はラベルを入力します。
12. 手順9でコピーしたファイルをUSBメモリにコピーしなおします。
13. ディスケットを取り出し、コンピュータを再起動します。USBメモリがCドライブとして起動されます。

デフォルトの起動順序はコンピュータによって異なり、コンピュータ セットアップ（F10）ユーティリティで変更することができます。

Windows 9xからDOSバージョンを使用した場合、短い間Windowsロゴの画面が表示されることがあります。表示されないようにするには、USBメモリのルート ディレクトリにLOGO.SYSというゼロ長のファイルを追加します。

13ページの「複数のコンピュータへのコピー」に戻ります。

サポートされないUSBフラッシュ メディア デバイス

注意：USBフラッシュ メディア デバイスから起動できないコンピュータもあります。コンピュータ セットアップ（F10）ユーティリティに表示されるデフォルトの起動順序で、USBデバイスがハードディスク ドライブより前にある場合、そのコンピュータはUSBフラッシュ メディア デバイスから起動できます。それ以外の場合は、起動可能ディスケットを使用してください。

起動可能なUSBフラッシュ メディア デバイスを作成するには、次のものが必要です。

- 次のうち1つのコンピュータ
  - Compaq Evo D510 US
  - Compaq Evo D510 MT/SF
  - HP Compaq Business Desktop d530シリーズ：US、SF、またはMT
  - Compaq Evo N400c、N410c、N600c、N610c、N620c、N800c、またはN1000cノートブック コンピュータ
  - Compaq Presario 1500または2800ノートブック コンピュータ

  BIOSによっては、将来リリースされるコンピュータでもUSBフラッシュ メディア デバイスからの起動がサポートされる場合があります。

注意：上記以外のコンピュータを使用している場合は、コンピュータ セットアップ（F10）ユーティリティに表示されるデフォルトの起動順序で、USBデバイスがハードディスク ドライブより前にあることを確認してください。

- FDISKおよびSYSプログラムが格納された、起動可能なDOSディスケット。SYSがない場合はFORMATを使用できますが、USBメモリ上のファイルがすべて失われます。

1. SCSI、ATA RAID、またはSATAドライブが取り付けられたPCIカードがコンピュータにある場合は、コンピュータの電源を切って電源コードを抜き取ります。

注意：電源コードは**必ず**抜き取ってください。

2. コンピュータのカバーを開いてPCIカードを取り外します。

3. USBフラッシュ メディア デバイスをコンピュータのUSBポートのどれかに差し込み、USBディスケット ドライブ以外のすべてのUSBストレージ デバイスを取り外します。コンピュータのカバーを閉じます。
4. 電源コードを差し込んでコンピュータの電源を入れます。モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押してコンピュータ セットアップ（F10）ユーティリティを起動します。
5. **[カスタム]**（Advanced）→**[PCIデバイス]**（PCI Devices）の順に選択してIDEおよびSATAコントローラを無効にします。SATAコントローラを無効にするとき、コントローラに割り当てられているIRQを書き留めておきます。後で再びIRQを割り当てる必要があります。変更を確定して、セットアップ ユーティリティを終了します。

   SATA IRQ：_____
6. FDISK.COMと、SYS.COMまたはFORMAT.COMのどちらかが格納された起動可能なDOSディスケットをディスケット ドライブに挿入します。コンピュータの電源を入れて、DOSディスケットを起動します。
7. FDISKを実行してUSBフラッシュ メディア デバイス上にあるパーティションをすべて削除します。新しいパーティションを作成して有効にします。**[Esc]**キーを押してFDISKを終了します。
8. FDISKを終了してもコンピュータが自動的に再起動されない場合は、**[Ctrl]**＋**[Alt]**＋**[Del]**キーを押して DOSディスケットから起動しなおします。
9. A:¥プロンプトで「**FORMAT C: /S**」と入力し、**[Enter]**キーを押します。FORMATによりUSBフラッシュ メディア デバイスがフォーマットされ、システム ファイルが追加され、ボリューム ラベルが要求されます。
10. ラベルを付けない場合は**[Enter]**キーを押し、必要な場合はラベルを入力します。
11. コンピュータの電源を切って電源コードを抜き取ります。コンピュータのカバーを開き、取り外しておいたPCIカードを取り付けなおします。コンピュータのカバーを閉じます。
12. 電源コードを差し込み、ディスケットを取り出してコンピュータの電源を入れます。
13. モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押してコンピュータ セットアップ（F10）ユーティリティを起動します。

14. **[カスタム]**（Advanced）→**[PCIデバイス]**（PCI Devices）の順に選択して、手順5で無効にしたIDEおよびSATAコントローラを再び有効にします。SATAコントローラを元のIRQに割り当てなおします。
15. 変更を保存してユーティリティを終了します。USBフラッシュ メディア デバイスがCドライブとして起動されます。

デフォルトの起動順序はコンピュータによって異なり、コンピュータ セットアップ（F10）ユーティリティで変更することができます。

Windows 9xからDOSバージョンを使用した場合、短い間Windowsロゴの画面が表示されることがあります。表示されないようにするには、USBメモリのルート ディレクトリにLOGO.SYSというゼロ長のファイルを追加します。

13ページの「複数のコンピュータへのコピー」に戻ります。

デュアル ステート電源ボタンの設定

お使いのコンピュータでWindows 2000、Windows XP Professional、またはWindows XP Home EditionのACPI（Advanced Configuration and Power Interface）を使用している場合は、電源ボタンをコンピュータのON/OFFとしての機能のほか、サスペンド モードを起動するためのボタンとして設定することができます。サスペンド モードでは、電源を完全に切らずに、コンピュータの消費電力を低い状態に保つことができます。使用中のアプリケーションを終了せずに作業を途中で中断したい場合など、サスペンド モードに設定しておくとコンピュータの電力を低く抑えることができます。

以下の手順に従って操作すると、電源ボタンを設定できます。

1. Windows 2000の場合：**[スタート]**ボタンを左クリックし、**[設定]→[コントロール パネル]→[電源オプション]**の順に選択します。

   Windows XP ProfessionalまたはWindows XP Home Editionの場合：**[スタート]**ボタンを左クリックし、**[コントロール パネル]→[パフォーマンスとメンテナンス]→[電源オプション]**の順に選択します。
2. **[電源オプションのプロパティ]**で、**[詳細]**（Windows 2000の場合）または**[詳細設定]**（Windows XPの場合）タブを選択します。
3. **[電源ボタン]**で、電源ボタンの設定を選択します。

電源ボタンをサスペンド モードに設定している場合は、コンピュータの電源が入っているときに電源ボタンを押すと、直ちにサスペンド モードを起動することができます。サスペンド モードから復帰する際も、電源ボタンを押します。電源ボタンをサスペンド モードに設定している場合にコンピュータの電源を切るには、電源ボタンを4秒以上押し続けます。

注意：システムが応答しない場合以外は、電源ボタンを使って電源を切らないでください。オペレーティング システムを通さずに電源を切ると、ハード ディスク ドライブが破損したりデータが損失したりする可能性があります。

インターネットWebサイト

HPの技術者がHP製および他社製のソフトウェアのテストおよび修正を行い、オペレーティング システムに特化したサポート ソフトウェアを開発しました。このため、HPのコンピュータは優れた性能、互換性、および信頼性を兼ね備えています。

別の種類のオペレーティング システムをインストールしたり新しいバージョンのオペレーティング システムに移行したりする場合、それぞれのオペレーティング システム用に設計されたサポート ソフトウェアを実行してください。お使いのコンピュータにインストールされているバージョンと異なるバージョンのMicrosoft Windowsを実行したい場合、対応するデバイス ドライバおよびユーティリティをインストールして、すべての機能がサポートされ、正しく動作することを確認してください。

HPでは、快適な環境で効率的にコンピュータをお使いいただくために、最新のデバイス ドライバ、ユーティリティ、フラッシュ ROMイメージなどを収録したサポート ソフトウェアを提供しています。サポート ソフトウェアはHPのWebサイト（http://www.hp.com/jp/support）からダウンロードできます。

HPのホームページには、HP製のコンピュータでMicrosoft Windowsのオペレーティング システムを使用する際に必要な最新のデバイス ドライバ、ユーティリティ、フラッシュ ROMイメージなどが用意されています。

標準規格およびパートナー企業

HPのインテリジェント マネジメント機能は、各社のシステム マネジメント アプリケーションを取り入れており、次のようなコンピュータ業界の標準規格に準拠しています。

- Desktop Management Interface（DMI）2.0
- Wake on LANテクノロジ
- ACPI
- SMBIOS
- Pre-boot Execution（PXE）サポート

資産情報管理機能およびセキュリティ機能

コンピュータに搭載される資産情報管理機能を使用すれば、HP Insightマネージャ、HP Client Manager、またはその他のシステム管理アプリケーションを使用して管理される資産情報を確認することができます。資産情報管理機能とこれらの管理ソフトウェア製品を統合することにより、お使いの環境に最適な管理ソフトウェアを選択でき、今までお使いになっていたソフトウェアをより有効に活用できます。

さらに、HPでは、コンピュータとデータを不正なアクセスから保護するための機能を備えています。HP ProtectTools内蔵セキュリティがインストールされている場合は、データへの不正なアクセスの防止、システムの整合性の確認、および第三者からのアクセスに対する認証が行われます。一部のモデルに装備されているProtectTools、スマート カバー センサ/カバー リムーバブル センサ（Cover Removable Sensor）、およびスマート カバー ロック（Smart Cover Lock）のようなセキュリティ機能は、コンピュータの内部装置への不正なアクセスの防止に役立ちます。パラレル ポート、シリアル ポート、またはUSBポートを無効にすることにより、またリムーバブル メディア ブート機能を無効にすることにより、貴重な資産であるデータを保護できます。これ以外にも、メモリ脱着センサおよびスマート カバー センサ/カバー リムーバブル センサからの警告が自動的にシステム管理アプリケーションに転送されることで、コンピュータの内部装置への不正なアクセスを防ぐことができます。

ProtectTools、スマート カバー センサ/カバー リムーバブル センサ、およびスマート カバー ロックは、一部のシステムにオプションとして装備されています。

次のユーティリティを使用して、セキュリティ機能の設定を管理できます。

- コンピュータ セットアップ（F10）ユーティリティを使用してローカルで管理します。コンピュータ セットアップ（F10）ユーティリティの詳しい情報と手順については、コンピュータに付属の『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください。

- HP Client ManagerまたはSystem Software Managerを使用してリモートで管理します。このソフトウェアにより、簡単なコマンドライン ユーティリティを使用して、ネットワークのセキュリティ機能の設定を確実に、一貫して集中管理することができます。

次の表と各項で、コンピュータ セットアップ（F10）ユーティリティを使ってローカルでコンピュータのセキュリティ機能を管理する方法を説明します。

セキュリティ機能

機能	目的	設定方法の概要
リムーバブル メディアからの起動（Removable Media Boot）制御	リムーバブル メディア ドライブからの起動を禁止する（一部のドライブのみ）	コンピュータ セットアップ（F10）ユーティリティを使う
シリアル ポート（ Serial Port）、パラレル ポート（ Parallel Port）、USBポート（ USB Port）、赤外線インターフェイス コント ロール（ Infrared Interface Control）制御	内蔵シリアル ポート、内蔵パラレル ポート、USBポート、および、オプションの外部赤外線トランシーバを使ったデータ転送を禁止する	コンピュータ セットアップ（F10）ユーティリティを使う
電源投入時パスワード（Power-On Password）	電源投入時および再起動時に、パスワードを入力するまでコンピュータを使用禁止にする	コンピュータ セットアップ（F10）ユーティリティを使う
セットアップ パスワード（Setup Password）	パスワードを入力するまでコンピュータ セットアップ ユーティリティを使ったコンピュータの設定の変更を禁止する	コンピュータ セットアップ（F10）ユーティリティを使う
内蔵セキュリティ デバイス（Embedded Security Device）	暗号化やパスワードでの保護によって、データへの不正なアクセスを防止する。システムの整合性を確認し、第三者からのアクセスを認証する	コンピュータ セットアップ（F10）ユーティリティを使う
ドライブロック（DriveLock）	マルチベイ ハードディスク ドライブにあるデータへの不正アクセスを禁止する（一部のモデルのみ）	コンピュータ セットアップ（F10）ユーティリティを使う

✎ コンピュータ セットアップについて詳しくは、『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください。サポートされるセキュリティ機能は、お使いのコンピュータの構成によって異なる場合があります。

セキュリティ機能（続き）

機能	目的	設定方法の概要
スマート カバー センサ (Smart Cover Sensor)	コンピュータ本体のカバーが取り外されたことを知らせる。カバーを取り外した後はセットアップ パスワードを入力するまでコンピュータを使用できないように設定することもできる。この機能について詳しくは、Documentation Library CD（ドキュメンテーション ライブラリCD）に収録されている『ハードウェア リファレンス ガイド』を参照	コンピュータ セットアップ（F10）ユーティリティを使う
マスタ ブート レコード セキュリティ（Master Boot Record Security）	現在の起動可能ディスクのマスタ ブート レコードを誤って変更したり、不正に変更したりできないようにする。また、正常であることがわかっている最新のマスタ ブート レコードを復元する	コンピュータ セットアップ（F10）ユーティリティを使う
メモリ脱着センサ (Memory Change Alerts)	メモリの脱着があったことを知らせる	設定方法などについては、オンライン ヘルプの「インテリジェント マネジメント機能」の説明を参照
オーナーシップ タグ (Ownership Tag)	コンピュータの起動時に所有者に関する情報を画面に表示する	コンピュータ セットアップ（F10）ユーティリティを使う
ケーブル ロック (Cable Lock Provision)	南京錠でコンピュータ本体のカバーを施錠して、コンピュータの設定を変更したり内部装置を取り外したりできないようにする 盗難防止ケーブルでコンピュータを固定して、無断で持ち出せないようにする セキュリティ ブラケットに南京錠を取り付けて、机などに固定する	セキュリティ ブラケットに市販の盗難防止ケーブルを取り付ける
セキュリティ ループ (Security Loop Provision)	コンピュータの設定を変更したり内部装置を取り外したりできないようにする	セキュリティ ループに錠を取り付け、コンピュータの設定を変更したり内部装置を取り外したりできないようにする

✎ コンピュータ セットアップについて詳しくは、『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください。サポートされるセキュリティ機能は、お使いのコンピュータの構成によって異なる場合があります。

パスワードのセキュリティ

電源投入時パスワード（Power-on password）は、コンピュータの電源を入れたり再起動するたびに、アプリケーションやデータにアクセスするためのパスワードの入力が要求されるので、コンピュータが許可無く使用されることを防ぎます。セットアップ パスワード（Setup password）は、特にコンピュータ セットアップ（F10）ユーティリティへの不正アクセスを防ぎます。セットアップ パスワードを、電源投入時パスワードの補助手段として使用することもできます。つまり、電源投入時パスワードの入力を要求されたときに、代わりにセットアップ パスワードを入力してコンピュータにアクセスすることもできます。

ネットワーク全体のセットアップ パスワードを設定しておくと、システム管理者はネットワーク上のすべてのシステムにログインでき、設定されている電源投入時パスワードを知らなくてもメンテナンスを行うことができます。

セットアップ パスワードの設定

システムに内蔵セキュリティ デバイスが搭載されている場合は、31ページの「内蔵セキュリティ」を参照してください。

[コンピュータ セットアップ（F10）ユーティリティ]メニューで、セットアップ パスワードを設定しておけば、無断でコンピュータの設定を変更されるのを防ぐことができます。

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]**→[OK]の順に選択して再起動します。
2. モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押します。必要であれば、**[Enter]**キーを押してタイトル画面を終了してください。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータの電源をいったん切ってから入れなおして、もう一度**[F10]**キーを押してください。

3. **[セキュリティ]**（Security）→**[セットアップ パスワード]**（Setup Password）の順に選択したあと、画面上のメッセージに従って操作します。
4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

電源投入時パスワードの設定

[コンピュータ セットアップ ユーティリティ]メニューで、電源投入時パスワードを設定しておけば、無断でコンピュータが使用されることを防止できます。電源投入時パスワードが設定されていると、コンピュータ セットアップ ユーティリティの**[セキュリティ設定]**（Security）メニューに**[パスワード オプション]**（Password options）が表示されます。パスワード オプションには**[ウォーム ブート時のパスワード入力]**（Password Prompt on Warm Boot）などが含まれます。**[ウォーム ブート時のパスワード入力]**が有効にされている場合も、コンピュータを再起動するたびにパスワードを入力する必要があります。

1. コンピュータの電源を入れるか、**[スタート]**→**[シャットダウン]**→**[再起動]**→[OK]の順に選択して再起動します。
2. モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押します。必要であれば、**[Enter]**キーを押してタイトル画面を終了してください。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータの電源をいったん切ってから入れなおして、もう一度**[F10]**キーを押してください。

3. **[セキュリティ]**→**[電源投入時パスワード]**（Power-On Password）の順に選択したあと、画面上のメッセージに従って操作します。
4. 設定を終了するには、**[ファイル]** →**[変更を保存して終了]** の順に選択します。

電源投入時パスワードの入力

電源投入時パスワードを入力するには、以下の手順で操作します。

1. コンピュータの電源を入れるか、**[スタート]**→**[シャットダウン]**→**[再起動]**→[OK]の順に選択して再起動します。
2. 鍵形のアイコンが表示されたら、パスワードを入力して**[Enter]**キーを押します。

機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

間違ったパスワードを入力した場合は、鍵形に×印のついたアイコンが表示されますので、パスワードを正しく入力しなおしてください。続けて3回間違えた場合は、コンピュータの電源をいったん切って最初から操作しなおす必要があります。

セットアップ パスワードの入力

システムに内蔵セキュリティ デバイスが搭載されている場合は、31ページの「内蔵セキュリティ」を参照してください。

コンピュータでセットアップ パスワードを設定しておけば、**[コンピュータ セットアップ ユーティリティ]**メニューを実行するたびに、必ずパスワードの入力が必要となります。

1. コンピュータの電源を入れるか、**[スタート]**→**[シャットダウン]**→**[再起動]**→[OK]の順に選択して再起動します。
2. モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押します。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータの電源をいったん切ってから入れなおして、もう一度**[F10]**キーを押してください。

3. 鍵形のアイコンが表示されたら、セットアップ パスワードを入力して**[Enter]**キーを押します。

機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

間違ったパスワードを入力した場合は、鍵形に×印のついたアイコンが表示されますので、パスワードを正しく入力しなおしてください。続けて3回間違えた場合は、コンピュータの電源をいったん切って最初から操作しなおす必要があります。

電源投入時パスワードまたはセットアップ パスワードの変更

システムに内蔵セキュリティ デバイスが搭載されている場合は、31ページの「内蔵セキュリティ」を参照してください。

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]→[OK]**の順に選択して再起動します。
2. 鍵形のアイコンが表示されたら、次のように入力します。

   現在のパスワード/新しいパスワード/新しいパスワード

機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

3. **[Enter]**キーを押します。

新しいパスワードは、次にコンピュータの電源を入れたときから有効になります。

電源投入時パスワードとセットアップ パスワードは、コンピュータ セットアップ（F10）ユーティリティの**[セキュリティ]**（Security）オプションを使って変更することもできます。

電源投入時パスワードまたはセットアップ パスワードの削除

システムに内蔵セキュリティ デバイスが搭載されている場合は、31ページの「内蔵セキュリティ」を参照してください。

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]→[OK]**の順に選択して再起動します。
2. 鍵形のアイコンが表示されたら、次のように入力します。

   現在のパスワード/

3. **[Enter]**キーを押します。

電源投入時パスワードとセットアップ パスワードは、コンピュータ セットアップ ユーティリティの**[セキュリティ]**（Security）オプションを使って変更することもできます。

電源投入時パスワードを忘れてしまった場合

設定しておいた電源投入時パスワードを忘れると、コンピュータを使用できなくなります。パスワードを解除する方法については、『トラブル シューティング ガイド』を参照してください。

システムに内蔵セキュリティ デバイスが搭載されている場合は、31ページの「内蔵セキュリティ」を参照してください。

内蔵セキュリティ

ProtectTools内蔵セキュリティでは、暗号化とパスワードによる保護を組み合わせて、暗号化ファイル システム（EFS）でのファイルやフォルダの暗号化によるセキュリティ機能を向上させます。また、Microsoft OutlookとOutlook Expressでの電子メールをセキュリティ保護します。ProtectToolsは一部のビジネス デスクトップ モデルでCTO（Configured-To-Order）オプションとして提供されます。データの漏えいを一番に心配され、データへの不正なアクセスがデータの損失よりはるかに危険であると考えるHPのお客様のための機能です。ProtectToolsでは4つのパスワードを使用します。

- （F10）Setup：コンピュータ セットアップ（F10）ユーティリティを起動して、ProtectToolsを有効または無効に設定するためのパスワードです。
- Take Ownership：ユーザを認証し、セキュリティのパラメータを設定するシステム管理者が設定および使用します。
- Emergency Recovery Token：システム管理者が設定します。コンピュータまたはProtectToolsチップの不具合の際にリカバリを許可します。
- Basic User：エンド ユーザが設定および使用します。

エンド ユーザのパスワードを忘れてしまうと、暗号化されたデータを復元できなくなります。このため、ユーザのドライブに含まれるデータをシステム情報のシステムに複製したり、定期的にバックアップを取ったりすることで、ProtectToolsを最も安全に使用できます。

ProtectTools内蔵セキュリティはTCPA 1.1に準拠したセキュリティ チップで、一部のビジネス デスクトップ コンピュータのシステム ボードにオプションで装備されています。ProtectTools内蔵セキュリティ チップは各コンピュータに固有のものです。それぞれのチップがコンピュータのその他のコンポーネント（プロセッサ、メモリ、オペレーティング システムなど）から独立したセキュリティ プロセスを実行します。

ProtectTools内蔵セキュリティが有効なコンピュータでは、Microsoft Windows 2000やWindows XP ProfessionalまたはHome Editionのセキュリティ機能が内蔵セキュリティで補完され、機能が向上します。たとえば、オペレーティング システムではローカルのファイルやフォルダがEFSに基づいて暗号化されますが、ProtectTools内蔵セキュリティではさらにセキュリティ機能が追加され、暗号化キーがプラットフォームのルート キー（シリコンに保存されています）から作成されます。このプロセスは暗号化キーの「ラッピング」と呼ばれます。ProtectToolsを使用していても、ProtectToolsを使用していないコンピュータへのネットワーク アクセスは可能です。

ProtectTools内蔵セキュリティの主な機能は、次のとおりです。

- プラットフォームの認証
- ストレージの保護
- データの整合性の確認

注意：パスワードは安全な場所に保管してください。**暗号化されたデータは、パスワードがないとアクセスしたり復元したりすることができません。**

パスワードの設定

Setup

Setupパスワードを作成して、コンピュータ セットアップ（F10）ユーティリティで内蔵セキュリティ デバイスを有効にできます。

1. モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押します。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータの電源をいったん切ってから入れなおして、もう一度**[F10]**キーを押してください。

2. 上下の矢印キーを使用して言語を選択し、**[Enter]**キーを押します。
3. 左右の矢印キーを使用して**[セキュリティ]**（Security）タブに移動し、上下の矢印キーを使用して**[セットアップ パスワード]**（Setup Password）に移動します。**[Enter]**キーを押します。

4. パスワードを入力して確定します。**[F10]** キーを押してパスワードを許可します。

機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

5. 上下の矢印キーを使用して[Embedded Security Device]（内蔵セキュリティ デバイス）に移動し、**[Enter]**キーを押します。
6. ダイアログ ボックスで[Embedded Security Device—Disable]（無効）が選択されている場合、左右の矢印キーを使用して[Embedded Security Device—Enable]（有効）に変更します。**[F10]**キーを押して変更を確定します。

注意：[Reset to Factory Settings—Reset]（リセット）を選択するとすべてのキーが消去され、キーのバックアップがない限り、暗号化されたデータを復元できなくなります（詳しくは、「Take Ownership と Emergency Recovery Token」を参照してください）。[Reset]は、暗号化されたデータを復元する手順で指示された場合にのみ選択します（36ページの「暗号化されたデータの復元」を参照してください）。

7. 左右の矢印キーを使用して**[ファイル]**（File）に移動します。上下の矢印キーを使用して**[変更を保存して終了]**（Save Changes and Exit）に移動します。**[Enter]**キーを押し、**[F10]**キーを押して変更を確定します。

Take OwnershipとEmergency Recovery Token

Take Ownershipパスワードは、セキュリティ プラットフォームを有効/無効に設定するとき、およびユーザを認証するときに必要です。内蔵セキュリティ デバイスに不具合が出た場合、Emergency Recovery機能によってユーザの認証やデータへのアクセスが可能になります。

1. Windows XP ProfessionalまたはHome Editionをお使いの場合は、**[スタート]→[すべてのプログラム]→**[HP ProtectTools Embedded Security Tools]（HP ProtectTools内蔵セキュリティ ツール）→[Embedded Security Initialization Wizard]（内蔵セキュリティ初期化ウィザード）の順に選択します。

   Windows 2000をお使いの場合は、**[スタート]→[プログラム]→**[HP ProtectTools Embedded Security Tools]→[Embedded Security Initialization Wizard]の順に選択します。

2. [Next]（次へ）をクリックします。
3. Take Ownershipパスワードを入力して確定し、[Next]をクリックします。

機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

4. [Next] をクリックしてデフォルトの Recovery アーカイブの場所を確定します。
5. Emergency Recovery Tokenパスワードを入力して確定し、[Next]をクリックします。
6. Emergency Recovery Tokenキーを格納するディスケットを挿入します。[Browse]（参照）をクリックしてディスケットを選択します。

注意：Emergency Recovery Tokenキーは、コンピュータや内蔵セキュリティ チップに不具合がある場合に、暗号化されたデータを復元するために使用します。**キーがないと、データを復元できません**（Basic Userパスワードがない場合にも、データにアクセスできません）。このディスケットは安全な場所に保管してください。

7. [Save]（保存）をクリックしてファイルの場所とデフォルトのファイル名を確定し、[Next]をクリックします。
8. [Next]をクリックして、セキュリティ プラットフォームが初期化される前に設定を確定します。

内蔵セキュリティ機能が初期化されていないというメッセージが表示される場合がありますが、これをクリックしないでください。このメッセージについては後の手順で説明します。メッセージは数秒後に閉じます。

9. [Next]をクリックしてローカル ポリシーの設定を省略します。
10. [Start Embedded Security User Initialization Wizard]（内蔵セキュリティ ユーザ初期化ウィザードを開始する）チェック ボックスが選択されていることを確認し、[Finish]（終了）をクリックします。

これで、[User Initialization Wizard]（ユーザ初期化ウィザード）が自動的に起動するようになります。

Basic User

ユーザ設定の初期化中にBasic Userパスワードが作成されます。このパスワードは、暗号化されたデータの入力やアクセスの際に必要です。

注意：Basic Userパスワードは安全な場所に保管してください。**暗号化されたデータは、このパスワードがないとアクセスしたり復元したりすることができません。**

1. [User Initialization Wizard]（ユーザ初期化ウィザード）が開いていない場合は、次のようにします。

   Windows XP ProfessionalまたはHome Editionをお使いの場合は、**[スタート]→[すべてのプログラム]→**[HP ProtectTools Embedded Security Tools]（HP ProtectTools内蔵セキュリティ ツール）→[User Initialization Wizard]の順に選択します。

   Windows 2000をお使いの場合は、**[スタート]→[プログラム]→**[HP ProtectTools Embedded Security Tools]→[User Initialization Wizard]の順に選択します。
2. [Next]（次へ）をクリックします。
3. Basic User Keyパスワードを入力して確定し、[Next]をクリックします。

機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

4. [Next]をクリックして設定を確定します。
5. [Security Features]（セキュリティ機能）から適切な項目を選択し、[Next]をクリックします。
6. 適切な電子メール クライアントをクリックして選択し、[Next]をクリックします。
7. [Next]をクリックして暗号化証明書を適用します。
8. [Next]をクリックして設定を確定します。
9. [Finish]（終了）をクリックします。
10. コンピュータを再起動します。

暗号化されたデータの復元

ProtectToolsチップを交換した後でデータを復元するには、次のものが必要です。

- SPEmRecToken.xml：Emergency Recovery Tokenキー
- SPEmRecArchive.xml : 隠しフォルダ。デフォルトの場所は、C:¥Documents and Settings¥All Users¥Application Data¥Infineon¥TPM Software¥Recovery Archive
- ProtectToolsパスワード
  - ❏ Setup
  - ❏ Take Ownership
  - ❏ Emergency Recovery Token
  - ❏ Basic User

1. コンピュータを再起動します。
2. モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押します。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータの電源をいったん切ってから入れなおして、もう一度**[F10]**キーを押してください。

3. Setupパスワードを入力して、**[Enter]**キーを押します。
4. 上下の矢印キーを使用して言語を選択し、**[Enter]**キーを押します。
5. 左右の矢印キーを使用して**[セキュリティ]**（Security）タブに移動し、上下の矢印キーを使用して[Embedded Security Device]（内蔵セキュリティ デバイス）に移動します。**[Enter]**キーを押します。
6. 選択肢が[Embedded Security Device—Disable]（無効）のみの場合、以下の操作を行います。
   a. 左右の矢印キーを使用して[Embedded Security Device—Enable]（有効）に変更します。**[F10]**キーを押して変更を確定します。
   b. 左右の矢印キーを使用して**[ファイル]**（File）に移動します。上下の矢印キーを使用して**[変更を保存して終了]**（Save Changes and Exit）に移動します。**[Enter]**キーを押し、**[F10]**キーを押して変更を確定します。
   c. 手順1に戻ります。

   選択肢が2つある場合は、手順7に進みます。

7. 上下の矢印キーを使用して[Reset to Factory Settings—Do Not Reset]（リセットしない）に移動します。左右の矢印キーを1回押します。

   [Performing this action will reset the embedded security device to factory settings if settings are saved on exit.]（こうすることにより、終了時に設定が保存されると、内蔵セキュリティ デバイスが工場出荷時の状態にリセットされることになります。）というメッセージが表示されます。任意のキーを押して続行します。

   [Enter]キーを押します。

8. 選択した項目が[Reset to Factory Settings—Reset]（リセット）に変更されます。**[F10]**キーを押して変更を確定します。
9. 左右の矢印キーを使用して**[ファイル]**（File）に移動します。上下の矢印キーを使用して**[変更を保存して終了]**（Save Changes and Exit）に移動します。**[Enter]**キーを押し、**[F10]**キーを押して変更を確定します。
10. コンピュータを再起動します。
11. モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押します。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータの電源をいったん切ってから入れなおして、もう一度**[F10]**キーを押してください。

12. Setupパスワードを入力して、**[Enter]**キーを押します。
13. 上下の矢印キーを使用して言語を選択し、**[Enter]**キーを押します。
14. 左右の矢印キーを使用して**[セキュリティ]**（Security）タブに移動し、上下の矢印キーを使用して[Embedded Security Device]（内蔵セキュリティ デバイス）に移動します。**[Enter]**キーを押します。
15. ダイアログ ボックスで[Embedded Security Device—Disable]（無効）が選択されている場合、左右の矢印キーを使用して[Embedded Security Device—Enable]（有効）に変更します。**[F10]**キーを押します。
16. 左右の矢印キーを使用して**[ファイル]**に移動します。上下の矢印キーを使用して**[変更を保存して終了]**に移動します。**[Enter]**キーを押し、**[F10]**キーを押して変更を確定します。
17. Windowsが起動したら、以下の操作を行います。

    Windows XP ProfessionalまたはHome Editionをお使いの場合は、**[スタート]→[すべてのプログラム]→**[HP ProtectTools Embedded Security Tools]（HP ProtectTools内蔵セキュリティ ツール）→[Embedded Security Initialization Wizard]（内蔵セキュリティ初期化ウィザード）の順に選択します。

Windows 2000をお使いの場合は、[スタート]→[プログラム]→[HP ProtectTools Embedded Security Tools]→[Embedded Security Initialization Wizard]の順に選択します。

18. [Next]（次へ）をクリックします。
19. Take Ownershipパスワードを入力して確定し、[Next]をクリックします。

機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

20. [Create a new recovery archive]（新規リカバリ アーカイブを作成）が選択されていることを確認します。[Recovery archive location]（リカバリ アーカイブの場所）の[Browse]（参照）をクリックします。
21. デフォルトのファイル名を確定しないでください。元のファイルを上書きしないために、新しいファイル名を入力します。
22. [Save]（保存）→[Next]の順に選択します。
23. Emergency Recovery Tokenパスワードを入力して確定し、[Next]をクリックします。
24. Emergency Recovery Tokenキーを格納するディスケットを挿入します。[Browse]をクリックしてディスケットを選択します。
25. デフォルトのキー名を確定しないでください。元のキーを上書きしないために、新しいキー名を入力します。
26. [Save]→[Next]の順に選択します。
27. [Next]をクリックして、セキュリティ プラットフォームが初期化される前に設定を確定します。

Basic Userキーをロードできないというメッセージが表示される場合がありますが、これをクリックしないでください。このメッセージについては後の手順で説明します。メッセージは数秒後に閉じます。

28. [Next]をクリックしてローカル ポリシーの設定を省略します。
29. [Start Embedded Security User Initialization Wizard]（内蔵セキュリティ ユーザ初期化ウィザードを開始する）チェック ボックスをクリックしてオフにし、[Finish]（終了）をクリックします。
30. ツールバーの[ProtectTools]を右クリックして、[Initialize Embedded Security restoration]（内蔵セキュリティ復元の初期化）をクリックします。

    これで[HP ProtectTools Embedded Security Initialization Wizard]（HP ProtectTools内蔵セキュリティ初期化ウィザード）が開始されます。

31. [Next]（次へ）をクリックします。
32. 元のEmergency Recovery Tokenキーが格納されているディスケットを挿入します。[Browse]（参照）をクリックし、トークンをダブルクリックしてフィールドに名前を入力します。デフォルトの名前はA:¥SPEmRecToken.xmlです。
33. 元のTokenパスワードを入力して[Next]をクリックします。
34. [Browse]をクリックし、元のRecovery Archiveをダブルクリックしてフィールドに名前を入力します。デフォルトの名前はC:¥Documents and Settings¥All Users¥Application Data¥Infineon¥TPM Software¥RecoveryArchive¥SPEmRecArchive.xmlです。
35. [Next]をクリックします。
36. 復元するコンピュータをクリックして、[Next]をクリックします。
37. [Next]をクリックして設定を確定します。
38. セキュリティ プラットフォームが復元されたというメッセージが表示されたら、手順39に進みます。

    復元が失敗したというメッセージが表示されたら、手順10に戻ります。パスワード、トークンの場所と名前、およびアーカイブの場所と名前をよく確認します。
39. [Finish]（終了）をクリックします。
40. Windows XP ProfessionalまたはHome Editionをお使いの場合は、[スタート]→[すべてのプログラム]→[HP ProtectTools Embedded Security Tools]（HP ProtectTools内蔵セキュリティ ツール）→[User Initialization Wizard]の順に選択します。

    Windows 2000をお使いの場合は、[スタート]→[プログラム]→[HP ProtectTools Embedded Security Tools]→[User Initialization Wizard]の順に選択します。
41. [Next]をクリックします。
42. [Recover your basic user key]（基本ユーザ キーの復旧）→[Next]の順に選択します。
43. ユーザを選択し、そのユーザの元のBasic Userキーのパスワードを入力して、[Next]をクリックします。
44. [Next] をクリックして設定を確定し、デフォルトの復元データの場所を確定します。

手順45～49を実行すると、元のBasic User設定が再インストールされます。

45. [Security Features]（セキュリティ機能）から適切な項目を選択し、[Next]（次へ）をクリックします。
46. 適切な電子メール クライアントをクリックして選択し、[Next]をクリックします。
47. 暗号化証明書をクリックし、[Next]をクリックして適用します。
48. [Next]をクリックして設定を確定します。
49. [Finish]（終了）をクリックします。
50. コンピュータを再起動します。

注意：Basic Userパスワードは安全な場所に保管してください。**暗号化されたデータは、このパスワードがないとアクセスしたり復元したりすることができません。**

ドライブロック（DriveLock）

ドライブロックは、マルチベイ ハードディスク ドライブにあるデータへの不正アクセスを禁止する業界標準のセキュリティ機能であり、コンピュータ セットアップ（F10）ユーティリティの拡張機能として実装されています。この機能は、ドライブロックが可能なハードディスク ドライブが検出された場合にのみ利用できます。

ドライブロックは、データのセキュリティを最重要視するユーザ向けに開発されました。このようなユーザにとっては、ハードディスク ドライブのコストとそこに格納されているデータの喪失は、データへの不正アクセスの結果生じる可能性のある損害に比べれば、些細なものです。このレベルのセキュリティを確保するのと同時に、パスワードを忘れたときの対処もできるように、HPが実装したドライブロックでは、2つのパスワードによるセキュリティ方式を採用しています。一方のパスワードはシステム管理者が設定し、使用するもので、もう一方のパスワードは通常、エンド ユーザが設定し、使用します。両方のパスワードを忘れてしまった場合にドライブをアンロックするための手段はありません。したがって、ハードディスク ドライブに含まれるデータが企業情報システムに複製されているか、または定期的にバックアップが作成されている場合に、ドライブロックを最も安全に使用できます。

ドライブロックの両方のパスワードを忘れてしまった場合は、ハードディスク ドライブを使用できなくなります。事前に定義されたカスタマ プロファイルに適合しないすべてのユーザにとって、この事実は受け入れ難いリスクになる可能性があります。一方、カスタマ プロファイルに適合するユーザにとっては、ハードディスク ドライブに保存されたデータの性質上、許容できるリスクだと言えます。

ドライブロックの使用法

[ドライブロック]（DriveLock）オプションは、コンピュータ セットアップ（F10）ユーティリティの**[セキュリティ]**（Security）メニューに表示されます。ユーザには、マスタ パスワード（master password）を設定したりドライブロックを有効にしたりするオプションが提供されます。ドライブロックを有効にするには、ユーザ パスワード（user password）を入力する必要があります。通常、ドライブロックの最初のコンフィギュレーションはシステム管理者が実行するので、マスタ パスワードが最初に設定されます。ドライブロックを有効にするか無効のままにしておくかにかかわらず、管理者はマスタ パスワードを設定することをお勧めします。これにより、将来ドライブがロックされた場合に、管理者はドライブロックの設定値を変更できるようになります。マスタ パスワードが設定されると、システム管理者はいつでもドライブロックを有効にしたり無効にしたりすることができます。

ロックされたハードディスク ドライブが存在する場合は、POST（Power-On Self Test）によって、そのドライブをアンロックするためのパスワードが要求されます。電源投入時パスワード（power-on password）が設定されていて、また、そのドライブのユーザ パスワードと一致する場合は、パスワードの再入力は要求されません。一致しない場合は、ドライブロックのパスワードを入力するよう要求されます。マスタ パスワードとユーザ パスワードのどちらを使うこともできます。ユーザは、パスワードが正しいと認識されるまで、2回入力できます。2回とも受け入れられない場合でもPOSTは続行されますが、そのドライブにはアクセスできません。

ドライブロックの使用例

ドライブロックのセキュリティ機能は、企業環境での使用に最も適しています。つまり、システム管理者が、ユーザに複数のコンピュータで使用できるようマルチベイ ハードディスク ドライブを提供する場合です。システム管理者はマルチベイ ハードディスク ドライブのコンフィギュレーションを担当しますが、その中で最も重要な作業は、ドライブロックのマスタ パスワードを設定することです。ユーザがユーザ パスワードを忘れた場合や、コンピュータを別の従業員が使うことになった場合、システム管理者はマスタ パスワードを使用して、ユーザ パスワードをリセットしたり、ハードディスク ドライブへのアクセス権を回復したりすることができます。

企業システム管理者は、ドライブロックを有効にする場合、マスタ パスワードの設定とメンテナンスについての企業方針を確立しておくことをお勧めします。こうすることで、従業員が会社を辞める前に意図的に、または誤ってドライブロックの両方のパスワードを設定してしまうという状況を防ぐことができます。両方のパスワードを設定した従業員が会社を辞めてしまった場合、そのハードディスク ドライブは使用不能となり、交換が必要になります。また、マスタ パスワードが設定されていないと、システム管理者がロックされたハードディスク ドライブにアクセスできなくなり、不正ソフトウェアの日常チェックや、その他の資産管理およびサポートを実行できなくなることがあります。

それほど厳重なセキュリティを必要としないユーザの場合は、ドライブロックを有効にしないことをお勧めします。この種のユーザには、個人ユーザや、機密性の高いデータをハードディスク ドライブに保持しないことを習慣にしているユーザが含まれます。このようなユーザにとっては、両方のパスワードを忘れてハードディスク ドライブ上のデータを失うことの損失のほうが、データを保護するために設計されたドライブロックの価値よりもはるかに大きいと言えます。コンピュータ セットアップ（F10）ユーティリティとドライブロックへのアクセスは、セットアップ パスワードによって制限できます。セットアップ パスワードを指定してそれをエンド ユーザに公表しないことで、システム管理者はユーザがドライブロックを有効にできないようにします。

スマート カバー センサ/カバー リムーバブル センサ（Cover Removable Sensor）

一部のモデルに搭載されているスマート カバー センサ/カバー リムーバブル センサとは、本体のカバーまたはサイド パネルの着脱があったことをユーザに知らせる、ハードウェア技術とソフトウェア技術を結合した機能です。3段階の設定レベルがあり、本体のカバーの着脱があった後で初めてコンピュータの電源を入れたときの動作が異なります。

スマート カバー センサ/カバー リムーバブル センサの動作

レベル	設定	コンピュータ起動時の動作
0	[無効]（Disabled）	スマート カバー センサ/カバー リムーバブル センサは無効（デフォルト）
1	[ユーザに通知]（Notify User）	本体のカバーが取り外されたことを知らせるメッセージが画面に表示される
2	[セットアップ パスワード]（Setup Password）	本体のカバーが取り外されたことを知らせるメッセージが画面に表示される セットアップ パスワードを入力するまで、コンピュータを使用できない

これらの設定は、コンピュータ セットアップを使用して変更できます。コンピュータ セットアップについて詳しくは、『コンピュータ セットアップ（F10）ユーティリティガイド』を参照してください。

スマート カバー センサ/カバー リムーバブル センサ（Cover Removable Sensor）の保護レベルの設定

以下の手順に従って、スマート カバー センサ/カバー リムーバブル センサ機能を有効にします。

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]→[OK]**の順に選択して再起動します。
2. モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押します。必要であれば、**[Enter]**キーを押してタイトル画面を終了してください。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータの電源をいったん切ってから入れなおして、もう一度**[F10]**キーを押してください。

3. **[セキュリティ]**（Security）→**[スマート カバー]**（Smart Cover）の順に選択したあと、画面上のメッセージに従って操作します。
4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

スマート カバー ロック

スマート カバー ロックは、一部のHPのコンピュータでサポートされるコンピュータのカバーのロックをソフトウェアで制御する機能です。スマート カバー ロックを使用して、コンピュータ内部の装置への不正なアクセスを防ぎます。工場出荷時には、ロックが解除された状態になっています。

注意:スマート カバー ロックを使用する場合は、必ずセットアップ パスワードを設定して、無断でロックを解除できないようにしておいてください。

スマート カバー ロックは、一部のシステムにオプションとして装備されています。

スマート カバー ロックの設定

以下の手順に従って、スマート カバー ロックを使って、コンピュータ本体のカバーをロックします。

1. コンピュータの電源を入れるか、**[スタート]**→**[シャットダウン]**→**[再起動]**→[OK]の順に選択して再起動します。
2. モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押します。必要であれば、**[Enter]**キーを押してタイトル画面を終了してください。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータの電源をいったん切ってから入れなおして、もう一度**[F10]**キーを押してください。

3. **[セキュリティ]**（Security）→**[スマート カバー]**（Smart Cover）→**[ロック]**（Locked）の順に選択します。
4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

スマート カバー ロックの解除

1. コンピュータの電源を入れるか、**[スタート]**→**[シャットダウン]**→**[再起動]**→[OK]の順に選択して再起動します。
2. モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押します。必要であれば、**[Enter]**キーを押してタイトル画面を終了してください。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータの電源をいったん切ってから入れなおして、もう一度**[F10]**キーを押してください。

3. **[セキュリティ]**→**[スマート カバー]**→**[アンロック]**（Unlocked）の順に選択します。
4. 設定を終了するには、**[ファイル]**→**[変更を保存して終了]**の順に選択します。

Smart Cover FailSafeキーの使用

スマート カバー ロックを使ってコンピュータをロックしたまま、パスワードを入力できなくなってしまった場合、Smart Cover FailSafeキーを使用して、コンピュータ本体のカバーを開ける必要があります。Smart Cover FailSafe キーが必要となるのは、次のような場合です。

- 停電
- 起動障害
- コンピュータ部品（プロセッサや電源など）障害
- パスワードを忘れてしまった場合

△ **注意：**Smart Cover FailSafeキーは、HPが提供する専用ツールです。必要になる前に、HP製品販売店であらかじめご用意いただくことをお勧めします。

Smart Cover FailSafeキーの入手については、HPのサポート窓口にお問い合わせください。

Smart Cover FailSafe キーについて詳しくは、『ハードウェア リファレンス ガイド』を参照してください。

マスタ ブート レコード セキュリティ（Master Boot Record Security）

マスタ ブート レコード（MBR）には、ディスクから正常に起動して、ディスク上に保存されているデータにアクセスするための情報が入っています。マスタ ブート レコードのセキュリティ機能によって、誤ってMBRを変更したり不正にMBRが変更される（一部のコンピュータ ウイルスによってデータが変更されたり、ディスク ユーティリティを誤って使用したりするなど）ことを防止できます。また、システムの再起動時にMBRへの変更が検出された場合、このセキュリティによって「正常であることが分かっている最新の」MBRを復元することができます。

MBRセキュリティを有効にするには、以下の手順に従って操作します。

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]→[OK]**の順に選択して再起動します。
2. モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押します。必要であれば、**[Enter]**キーを押してタイトル画面を終了してください。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータの電源をいったん切ってから入れなおして、もう一度**[F10]**キーを押してください。

3. **[セキュリティ]**（Security）→**[マスタ ブート レコード セキュリティ]**（Master Boot Record Security）→**[有効]**（Enabled）の順に選択します。
4. **[セキュリティ]→[マスタ ブート レコードの保存]**（Save Master Boot Record）の順に選択します。
5. 設定を終了するには、**[ファイル]→[変更を保存して終了]**の順に選択します。

MBRセキュリティを有効にすると、BIOSは、MS-DOSやWindowsのSafeモードで現在の起動可能ディスクのMBRが変更されることを防ぎます。

ほとんどのオペレーティング システムは、現在の起動可能ディスクのMBRへのアクセスを制御します。したがって、オペレーティング システムの動作中に行われる変更については、BIOSは阻止できません。

コンピュータの電源を入れるか、再起動するたびに、BIOSは現在の起動可能ディスクのMBRと前回に保存されたMBRとを比較します。変更が検出され、かつ現在の起動可能ディスクが、前回MBRを保存したディスクと同じである場合、次のメッセージが表示されます。

1999 - Master Boot Record has changed.（マスタ ブート レコードが変更されました。）

Press any key to enter Setup to configure MBR Security（任意のキーを押して**[コンピュータ セットアップ ユーティリティ]**メニューで、MBRセキュリティを設定してください。）

[コンピュータ セットアップ ユーティリティ]メニューで、次の操作を行います。

- 現在の起動可能ディスクのMBRを保存します。
- 前回保存したMBRを復元します。または、
- MBRセキュリティ機能を無効にします。

セットアップ パスワードが設定されている場合は、セットアップ パスワードの入力が必要です。

変更が検出され、現在の起動可能ディスクが、前回にMBRを保存したディスクと同じでない場合は、次のメッセージが表示されます。

2000 - Master Boot Record Hard Drive has changed.（マスタ ブート レコードのハードディスク ドライブが変更されています。）

Press any key to enter Setup to configure MBR Security（任意のキーを押して**[コンピュータ セットアップ ユーティリティ]**メニューで、MBRセキュリティを設定してください。）

[コンピュータ セットアップ ユーティリティ]メニューで、次の操作を行います。

- 現在の起動可能ディスクのMBRを保存します。または、
- MBRセキュリティ機能を無効にします。

セットアップ パスワードが設定されている場合は、セットアップ パスワードの入力が必要です。

万一、前回保存したMBRが破損した場合は、次のメッセージが表示されます。

1998 - Master Boot Record has been lost.（マスタ ブート レコードがありません。）

Press any key to enter Setup to configure MBR Security（任意のキーを押して**[コンピュータ セットアップ ユーティリティ]**メニューで、MBRセキュリティを設定してください。）

[コンピュータ セットアップ ユーティリティ]メニューで、次の操作を行います。

- 現在の起動可能ディスクのMBRを保存します。または、
- MBRセキュリティ機能を無効にします。

セットアップ パスワードが設定されている場合は、セットアップ パスワードの入力が必要です。

現在の起動可能ディスクのパーティションとフォーマットを変更する前に

現在の起動可能ディスクのパーティションやフォーマットを変更する前に、MBRセキュリティが無効になっていることを確認してください。FDISKやFORMATなど一部のディスク ユーティリティは、MBRを更新しようとします。ディスクのパーティションやフォーマットを変更する際にMBRセキュリティが有効である場合は、次にコンピュータの電源を入れるか再起動したときに、ディスク ユーティリティからエラー メッセージが表示されたり、MBRセキュリティから警告が発生したりする可能性があります。MBRセキュリティを無効にするには、以下の手順に従って操作します。

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]→[OK]**の順に選択して再起動します。
2. モニタ ランプが緑色に点灯したら、すぐに**[F10]**キーを押します。必要であれば、**[Enter]**キーを押してタイトル画面を終了してください。

適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータの電源をいったん切ってから入れなおして、もう一度**[F10]**キーを押してください。

3. **[セキュリティ]**（Security）→**[マスタ ブート レコード セキュリティ]**（Master Boot Record Security）→**[無効]**（Disabled）の順に選択します。
4. 設定を終了するには、**[ファイル]→[変更を保存して終了]**の順に選択します。

ケーブル ロックの取り付け

コンピュータのリア パネルにはケーブル ロックを取り付けられるようになっているので、市販のケーブル ロックを使用して、コンピュータを作業エリアに固定できます。

詳しくは、Documentation Library CDに収録されている『ハードウェア リファレンス ガイド』を参照してください。

指紋認証テクノロジ

HP指紋認証テクノロジを使用すると、エンド ユーザのパスワードの入力が不要となるため、ネットワークのセキュリティを強化する一方で、ログイン手順を簡素化し、企業のネットワーク管理に関わる経費を削減することができます。また、手頃な価格のため、もはや一部のハイテク産業や高度なセキュリティを扱う組織や企業だけのものではなくなりました。

モデルによっては、指紋認証テクノロジがサポートされていない場合があります。

詳しくは、次のWebサイト（英語サイト）を参照してください。

http://h18000.www1.hp.com/solutions/security

障害通知および復旧機能

障害通知および復旧機能とは、最新のハードウェア/ソフトウェア技術を結合して、重要なデータの損失を防ぎ、故障時間を最小限に抑える機能です。

障害が発生すると、障害内容と対処方法を示した警告メッセージが画面上に表示されます。また、HP Client Managerを使用すれば、いつでもシステムの状態を調べることができます。HP Insightマネージャ、HP Client Manager、またはその他のシステム管理アプリケーションによって管理されるネットワークにコンピュータが接続されている場合は、ネットワーク管理ソフトウェアにも障害通知が送られます。

ドライブ保護システム

ドライブ保護システム（DPS）は、一部のモデルに搭載されたコンピュータのハードディスク ドライブに組み込まれている診断ツールです。DPSを使用して、ハードディスクの交換時に発生する問題を診断します。

コンピュータにハードディスク ドライブを取り付ける際にDPSテストを実行し、主要な情報をハードディスク ドライブに書き込みます。この情報は半永久的に記録されます。DPSを実行するたびに、テストの結果がハードディスク ドライブに書き込まれます。HPのサポート窓口はこの情報を使用して問題の原因を診断します。DPSの使用手順については『トラブルシューティング ガイド』を参照してください。

耐サージ機能付連続供給電源装置

耐サージ機能が付いた連続供給電源によって、急激な電圧の変化に対処することができます。この電源装置は、2000 Vまでのサージ電圧に耐え、データの損失やシステム ダウンを引き起こさないことが確認されています。

温度センサ機能

温度センサ機能は、ハードウェアとソフトウェアの統合により提供される機能で、コンピュータ内部の温度を監視し、コンピュータ内部の温度が通常の範囲を超えると、画面上に警告メッセージを表示します。これにより、内部部品の故障やデータの損失が発生する前に対処することができます。

モデルにより温度センサ機能はサポートされない場合があります。

索引